UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/525,605	04/15/2005	Seppo Keronen	IPT-15970	7979

40854 7590 09/24/2008

RANKIN, HILL & CLARK LLP
38210 Glenn Avenue
WILLOUGHBY, OH 44094-7808

EXAMINER	
PARK, JEONG S	

ART UNIT	PAPER NUMBER
2154	

MAIL DATE	DELIVERY MODE
09/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/525,605	KERONEN, SEPPO	
	Examiner	Art Unit	
	JEONG S. PARK	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 February 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/25/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claims 1-47 are objected to because of the following informalities:

In claim 1, line 5, the word "authorised" should be corrected as –authorized--. Similar correction should be made for claims 29, 44 and 46;

In claim 2, line 1, the word "a server" should be corrected as –the server-- for clear understanding of the claim. Similar correction should be made for claims 3-28;

In claim 30, line 1, the word "a terminal" should be corrected as –the terminal-- for clear understanding of the claim. Similar correction should be made for claims 31-43; and

In claim 45, line 1, the word "a method" should be corrected as –the method-- for clear understanding of the claim. Similar correction should be made for claim 47.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Valencia (U.S. Patent No. 6,308,213 B1).

Regarding claim 1, Valencia teaches as follows:

a server(interpreted as home gateway 20 in figure 2 and/or network access

server (hereinafter NAS) 27 in figure 2) network access server for allowing a user to connect to services (access to resources through LAN 22 in figure 2) using a remote terminal (remote client 26 in figure 2), the server being coupled to the remote terminal via one of a number of communications links (Internet 18 in figure 2) and to the one or more services in use (remote client gets access to the LAN for resources through the home gateway via the Internet, see, e.g., col. 3, line 43 to col. 4, line 3 and figure 2), the server including:

a store for storing device data (remote client's username and password), the device data including an indication of an identifier for each of a number of predetermined terminals authorized to access the remote services (NAS forwards authentication information to the home gateway, see, e.g., col. 6, line 46-56 and the home gateway memory (20 in figure 8) stores the client information, see, e.g., col. 7, lines 22-34);

an authentication system, the authentication system being adapted to obtain an identifier from the terminal, compare the identifier of the terminal to the device data (NAS authenticates the client using an authentication protocol CHAP which are well-known to those skilled in the art, see, e.g., col. 4, lines 52-59 and figure 4 steps 42), and establish a connection between the server and the terminal via at least one of the communication links (among existing tunnels), in response to the successful comparison (initiating a tunnel connection to the home gateway at step 50 using the authentication information gathered by the NAS in step 42 and establish a virtual dial-up session in step 61, see, e.g., col. 5, lines 1-24);

a cache store (interpreted as a memory in NAS 27 and home gateway 20 in figure 3) including a first cache adapted to store data transmitted to the terminal and a second cache adapted to store data received from the terminal (steps 1-5 in figure 8 describes communicating data between remote client and home gateway via NAS, see, e.g., col. 7, lines 1-34, therefore it is inherent to store the transmitted and received data in the memory at NAS and home gateway). It would be obvious to assign separate cache area for transmitted data to the remote client and for received data from the remote client;

a switching system, the switching system being adapted to receive an alternative connection request from the terminal (NAS determines whether the remote clients is requesting virtual dial-up service or standard dial-up service to a local network, see, e.g., col. 2, lines 3-9), the alternative connection request indicating that an alternative connection is to be established and cooperate with the terminal to establish the alternative connection in response to the request (the alternative connection request from remote client is established between the NAS and the home gateway, see, e.g., col. 2, lines 33-44); and

a security system (remote client authentication, see, e.g., col. 6, lines 46-67), the security system being adapted to perform at least one of encoding data to be transmitted to the terminal in accordance with the data stored in the cache store or decoding data received from the terminal in accordance with the data stored in the cache store (the home gateway encrypts the random number R according to the client

password which is prestored in the home gateway database, see, e.g., col. 7, lines 22-34).

Regarding claims 2 and 3, Valencia teaches that the security system (remote client authentication, see, e.g., col. 6, line 46 to col. 7, line 34) being adapted to encode data by compressing and then encrypting the data (see, e.g., col. 7, lines 9-34) and being adapted to decode data by decrypting and then decompressing the data. Also the encoding/decoding and compression/decompression method are well-known is the art.

Regarding claim 4, Valencia teaches that the terminal having a corresponding cache store, the corresponding cache store being adapted to be identical to the cache store (NAS, home gateway and remote client have a memory stored the same remote client data such as username and password, see, e.g., col. 2, lines 34-44).

Regarding claim 5, Valencia teaches that each cache and corresponding cache being adapted to store predetermined secret data (random number R according to the client password which is prestored in the home gateway database, see, e.g., col. 7, lines 9-34).

Regarding claim 6, Valencia teaches as follows:

comparing the data to be transferred (random number encrypted by remote client) to the data stored in the first cache (random number encrypted by home gateway), determining matching data in accordance with the results of the comparison (see, e.g., col. 7, lines 22-34) and modifying the data to be transmitted by replacing the matching data with a cache reference, the terminal being adapted to be responsive to the transmitted data to replace the cache references with the matching data from the

corresponding first cache (remote client replaces any current random number with the random number sent from NAS, see, e.g., step 2, col. 7, lines 1-8).

Regarding claim 7, Valencia teaches as follows:

locating cache references in the received data (step 2 in figure 8), the cache references being generated by the terminal (the encryption of random number) in accordance with data contained in the corresponding second cache (random number generated and stored at NAS)(remote client generates the encryption of random number according to the password using CHAP algorithm, see, e.g., col. 7, lines 9-21);

accessing the data stored in the second cache (random number stored at NAS); and

modifying the received data by replacing the cache references with matching data with a cache store reference, the terminal including a corresponding cache store and being adapted to be responsive to the transmitted data to replace the cache store references with the matching data from the corresponding cache store (remote client replaces any current random number with the random number sent from NAS, see, e.g., step 2, col. 7, lines 1-8).

Regarding claim 8, Valencia teaches as follows:

generating an encryption/decryption factor (secret) in accordance with the selected data stored in the cache store (password is a shared secret between remote client and home gateway, see, e.g., col. 7, lines 9-12); and

Encrypting/decrypting the compressed data in accordance with the generated

encryption/decryption factor (encryption of random number according to the password, see, e.g., col. 7, lines 1-21).

Regarding claim 9, Valencia teaches as follows:

the encryption/decryption factor being based on a checksum of the data contained in the first/second cache (packet checksum, see, e.g., col. 9, lines 19-28).

Regarding claim 10, Valencia teaches as follows:

the encryption/decryption factor (password) being used to generate an encryption/decryption key (encryption of random number according to the password), the key being used in a encryption/decryption algorithm (CHAP algorithm, see, e.g., col. 7, lines 9-21 and RFC 1994).

4. Claims 11-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Valencia (U.S. Patent No. 6,308,213 B1) in view of Yamanaka (hereinafter Yamanaka)(U.S. Patent No. 5,504,741).

Regarding claims 11 and 12, Valencia teaches all limitations of claim as presented above per claims 1-10 except for selecting the data in accordance with a priority requirements for the data transmission.

Yamanaka teaches that memory means may store the destination information and the priority and the search and select means may search the destination information for selecting data based on the stored priority (see, e.g., col. 5, lines 6-12).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Valencia to include selecting transmission data based on the priority as taught by Yamanaka in order to efficiently transmit the priority data.

Also the selecting transmission data based on transmission capacity, data volume, QoS requirements, or priority requirements are well-known to those skilled in the art.

Regarding claim 13, Valencia teaches the connection links including an Internet connection (Internet 18 in figure 2).

Regarding claim 14, Valencia teaches that at least one of the communications links being established as a tunnel connection with the terminal (initiate tunnel connection 50 in figure 4).

Regarding claim 15, Valencia teaches as follows:

the store being adapted to store user data, the user data including a user identifier for each user authorized to access the remote services, the authentication system being adapted to receive a user identifier from the terminal, compare the user identifier to the user data and establish the connection in response to a successful comparison (NAS authenticates the client using an authentication protocol CHAP which are well-known to those skilled in the art, see, e.g., col. 4, lines 52-59 and figure 4 steps 42, initiating a tunnel connection to the home gateway at step 50 using the authentication information gathered by the NAS in step 42 and establish a virtual dial-up session in step 61, see, e.g., col. 5, lines 1-24).

Regarding claim 16, Valencia teaches that the unique identifier being a username and password (see, e.g., col. 2, lines 33-45).

Regarding claim 17, Valencia teaches as follows:

the authentication system and the switching system being adapted to provide

one time authentication such that the unique identifier is not required when an alternative connection is to be established (home gateway uses the authentication information collected from NAS to complete remote client authentication avoiding an additional cycle of authentication, see, e.g., col. 5, lines 25-36).

Regarding claim 18, Valencia teaches as follows:

the cache store (a cache store interpreted as a memory in NAS 27 and home gateway 20 in figure 3) including a number of first and second caches, at least one respective first and second cache being used for each terminal adapted to be connected to the server (steps 1-5 in figure 8 describes communicating data between remote client and home gateway via NAS, see, e.g., col. 7, lines 1-34, therefore it is inherent to store the transmitted and received data in the memory at NAS and home gateway. It would be obvious to assign separate cache area for transmitted data to the remote client and for received data from the remote client).

Regarding claim 19, Valencia teaches as follows:

the connection being used to transfer a number of different data types (PPP frame and L2F frame), a respective first and second cache being used for each data type (NAS receives L2F frame to be transferred to the remote client and PPP frame from the remote client, see, e.g., col. 4, lines 4-13 and figure 2).

Regarding claim 20, Valencia teaches as follows:

the server (NAS) including a converter, the converter being adapted to receive data having a first form and output data having a second form (NAS converts between PPP and L2F protocols, see, e.g., col. 5, line 58-67 and figure 7).

Regarding claim 21, Valencia teaches that the converter (NAS) being accepted to receive UDP data from the Internet and transfer the data to the terminal as TCP data (see, e.g., col. 4, lines 24-28).

Regarding claim 22, Valencia teaches the authentication system as presented above per claim 1. It would be obvious to use digital signature as a secret key because Valencia teaches using a password as the secret key (password is a shared secret between remote client and home gateway, see, e.g., col. 7, lines 9-12).

Regarding claim 23, Valencia teaches as follows:

the predetermined information being obtained from the cache store (NAS, home gateway and remote client have a memory stored the same remote client data such as username and password, see, e.g., col. 2, lines 34-44).

Regarding claim 24, Valencia teaches as follows:

NAS (applicant's server) receives L2F frame to be transferred to the remote client and PPP frame from the remote client, see, e.g., col. 4, lines 4-13 and figure 2); and

NAS converts between PPP and L2F protocols (see, e.g., col. 5, line 58-67 and figure 7).

Therefore, the applicant's first address is equivalent to L2F protocol address and the applicant's second address is equivalent to PPP protocol address.

Regarding claim 25, Valencia teaches as follows:

determine alterations of the first address of the terminal (NAS converts between PPP and L2F protocols, see, e.g., col. 5, line 58-67 and figure 7).

5. Claims 29-38, 44 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Valencia (U.S. Patent No. 6,308,213 B1) in view of Kikuchi (U.S. Patent No. 6,446,132 B1).

Regarding claims 29, 44 and 46, Valencia teaches all limitations of claim as presented above per claim 1 except for comparing the alternative connection to the existing connection.

Kikuchi teaches as follows:

comparing each transmission time through the current and the alternative path with each other (see, e.g., abstract); and

when the transmission time through the alternative path is shorter than the through the current path, the current path is switched to the alternative path (see, e.g., abstract).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Valencia to include comparing a current path with a alternative path as taught by Kikuchi in order to reduce a communication charge and transmission time by switching to the alternative path before failure of the current path.

Regarding claim 30, Valencia in view of Kikuchi teach all limitations of claims as presented above per claims 1 and 29

Regarding claims 31, 32 and 34-38, Valencia in view of Kikuchi teach all limitations of claims as presented above per claims 1, 4-10 and 29.

Regarding claim 33, Kikuchi teaches as follows:

comparing each transmission time (equivalent to applicant's connection speed) through the current and the alternative path with each other (see, e.g., abstract).

Therefore claim 33 is rejected with the same reason as presented above per claim 29.

6. Claims 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Valencia (U.S. Patent No. 6,308,213 B1) in view of Yamanaka, and further in view of Kikuchi (U.S. Patent No. 6,446,132 B1).

Regarding claim 26, Valencia in view of Yamanaka teach all limitations of claim except for detecting failure of the established connection between the server and the terminal.

Kikuchi teaches that detection of failure (see, e.g., col. 2, line 19-23).

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Valencia in view of Yamanaka to include detecting path failure as taught by Kikuchi in order to efficiently manage current path and provide alternative path between a server and a terminal when detects a failure of the current path.

Regarding claims 27 and 28, Valencia in view of Yamanaka and further in view of Kikuchi teach all the limitations of claim as presented above per claims 1 and 26.

7. Claims 39-43, 45 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Valencia (U.S. Patent No. 6,308,213 B1) in view of Kikuchi (U.S. Patent No. 6,446,132 B1), and further in view of Yamanaka (hereinafter Yamanaka)(U.S. Patent No. 5,504,741).

Regarding claims 39 and 40, Valencia in view Kikuchi and further in view of Yamanaka teach all limitation as presented above per claims 11 and 12.

Regarding claims 41 and 42, Valencia in view Kikuchi and further in view of Yamanaka teach all limitations of claims as presented above per claims 13, 14 and 29.

Regarding claim 43, Valencia in view Kikuchi and further in view of Yamanaka teach all limitations of claims as presented above per claims 1 and 29

Regarding claim 45, Valencia in view Kikuchi and further in view of Yamanaka teach all limitations of claims as presented above per claims 1 and 44.

Regarding claim 47, Valencia in view Kikuchi and further in view of Yamanaka teach all limitations of claims as presented above per claims 29 and 46.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEONG S. PARK whose telephone number is (571)270-1597. The examiner can normally be reached on Monday through Friday 7:00 - 3:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. S. P./
Examiner, Art Unit 2154

September 19, 2008

/Joseph E. Avellino/
Primary Examiner, Art Unit 2146